EXAMINER'S AMENDMENT

Status of Claims

1. Claims 1, 3, 5-20, 22 and 24 have been cancelled. Claim 25 has been added. Claims 2, 21 and 23 are being amended.

2. The amendment filed on 15 October 2009 will not be entered.

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Eric Baron, Applicant's Representative on 21 January, 2010.

4. Claims 2, 4, 21, 23 and 25 are allowed.

Amend claim 2 as follows:

(currently amended) The improved method according to claim [[1]] 25, wherein the step of verifying comprises the step of:

verifying that a first value is derived from a base value included in the first set of signature values, is identical with a second value that is obtained from the base value, and is included in the second set of signature values.

Amend claim 21 as follows:

(currently amended) The improved method of claim [[1]] 25, wherein the hash is not forwarded to the security module in the user device.

Amend claim 23 as follows:

(currently amended) The improved method of claim [[1]] 25, wherein the second set of attestation values is usable by the user device only once and only with the verification computer.

Add claim 25 as follows:

(new) An improved method of maintaining privacy for transactions employing a user device having a security module, wherein the improvement comprises the steps of:

sending, by an issuer computer, an endorsement key to a user device, wherein the endorsement key is unique to the user device;

computing a hash of the endorsement key by the issuer computer and sending by the issuer computer, a first set of attestation values to the user device, wherein the first set of attestation values comprises the hash;

receiving, by a privacy computer, a first set of signature values from the user device, wherein the first set of signature values is a function of the first set of attestation values;

providing, by the privacy computer, a second set of attestation values to the user device, wherein the second set of attestation values are a function of the hash

receiving, by the verification computer the first set of signature values and a second set of signature values from the user device, wherein the second set of signature values is a function of the hash;

verifying, by the verification computer, that the first set of signature values and the second set of signature values are based on the hash; and

and based on the verifying step, providing, by the verification computer, access to a service, data, or information to the user device.

Reasons for Allowance

5. The following is an examiner's statement of reasons for allowance:

6. TPM (TPM Main Part 1 Design Principles, Specification Version 1.2, Revision 62, 2 October 2003, 161 pages, Trusted Computing Group) and TPM changes (TPM v1.2 Specification Changes, A summary of changes with respect to the v1.1b TPM Specification, October 2003, Trusted Computing Group, 14 pages,) teach the issuer computer sending attestation values to the user device and the user device sending a set of signature values based on the issuer attestation values to a verification computer. However neither TPM nor TPM changes alone or in combination specifically disclose the issuer computer sending an endorsement key to the user device, wherein the endorsement key is unique to the user device, computing a hash of the endorsement key and including the hash with the attestation values sent to the user device, the user device also receiving attestation values from a privacy computer and that the user device computes signature values for both the issuer attestation values and the privacy computer, with both sets of attestation values based on the issuer computed hash and that the user device is provided access to a service, data, or information based on a verification computer verifying that both signatures were based on the hash.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Camenisch et al. (WO2002042935) teaches providing anonymous access to a service within a network.
- TPM Main Part 1 Design Principles, Specification Version 1.2, Revision 62, 2 October 2003, 161 pages, Trusted Computing Group, discloses the operation of the trusted platform module as known at the time of Applicant's invention.
- TPM v1.2 Specification Changes, A summary of changes with respect to the v1.1b TPM Specification, October 2003, Trusted Computing Group, 14 pages also discloses the operation of the trusted platform module as known at the time of Applicant's invention.
- "A Signature Scheme with Efficient Protocols" (A Signature Scheme with Efficient Protocols", Camenisch and Lysyanskaya, date shown by file properties as 10/11/2002, 22 pages) discusses at length signatures employing zero-knowledge proofs.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D. NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on Monday-Thursday 6:45-5:15.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt II can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAMES D NIGH/
Examiner, Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685